… Coming to an Online Bank Near You!

John C. Checco, CISSP

Most information security professionals in the financial industry have already heard about the FFIEC (Federal Financial Institutions Examination Council) recommendation that all financial institutions have multi-factor authentication for internet-based services. What are the real implications of such a guideline? What are the ramifications of non-compliance? What technologies, techniques and procedures support these guidelines? And finally, what is the feasibility and cost-effectiveness to adhere to these guidelines?

The FFIEC Report

The FFIEC has proven to be an essential driver for defining sound methods and procedures in the financial industry, so it pays to listen before recommendations become regulations.

The FFIEC is a "formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions."[1] The agencies that comprise the FFIEC include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

This organization provides many guidelines to assist financial institutions in developing sound methods and procedures. Especially of interest are the Information Technology Examination Handbooks which include online booklets on BCP, e-Banking, Information Security, Outsourcing Technology Services, and a host of other best practices. Each booklet covers the theory, operational checklist, as well as legal and other external issues that affect the sanctity of doing business in the financial industry.

The FFIEC also publishes less-detailed guidances which recommend methods and procedures. One such guidance, Authentication in an Internet Banking Environment (10/12/2005), upon which this article focuses, strongly states that "the agencies consider single-factor authentication… to be inadequate" and "the authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services." The report details their findings and cross references its recommendations with existing regulations, such as the Interagency Guidelines Establishing Information Security Standards, Gramm-Leach-Bliley Act as well as the USA PATRIOT Act. In addition to the front-end authentication, the report also stresses the importance of monitoring and audit logs for mitigating fraud and identity theft.

[1] Source: http://www.ffiec.gov

The Onus of Implementation

Without clearly defined legal accountability and stiff financial penalties, there is no ROI for implementing the FFIEC recommendations.

Although the FFIEC states that "financial institutions should use this guidance when evaluating and implementing authentication systems and practices," this report lacks a definitive timeline for financial institutions to act as well as the repercussions of choosing to do business-as-usual. In fact, financial institutions are only liable for identity theft or credit card fraud committed through their internet-based services if the financial institutions fail to "implement reasonable physical, technical, and procedural safeguards to protect customer information[2]," However, because the FTC has never defined "reasonable measures," the existing practice of simple single-factor authentication can be considered reasonable and sufficient; hence, there is little motivation to pony up the monies for additional authentication procedures in an ever-tightening IT development environment.

The Character of Your Organization

The culture of an organization determines the breadth and depth of its risk mitigation implementation.

Feasibility, in traditional corporate terms, is the compromise between profits and costs. Feasibility, in the new information security landscape, is another term for risk mitigation – how much is your company willing to put its image and financial base at risk for each information security breach? Does your organization spend just as much on servicing the 50,000 SMB customers that only bring in $5B annually as it does for the top 100 Enterprise customers that bring in $15TR annually? What is your organization ready to spend on protecting the 500,000 online users in those 50,000 SMB customers versus the 10,000 online users in the top 100 Enterprise customers? In this article, feasibility refers to the cost-effectiveness of bringing multi-factor authentication to online customers that are below the profitable margin level those corporations usually give the most attention to. You need to examine your organization's culture to know what that price tag is.

The Suggested Possibilities

Multi-factor authentication has conventionally been a business decision that weighs risk avoidance against the rate of discontented clientele.

The appendix to this FFIEC report specifies many different possibilities for what constitutes appropriate multi-factor authentication, although the organization could have provided the relative costs and difficulty in the design, deployment and maintenance for each. Notably, some of the more effective techniques are not necessarily the most high-tech. All of the possibilities

[2] Source: "FTC Testifies on Data Security and Identity Theft" (ref . www.ftc.gov/opa/2005/06/datasectest.htm)

provided in the report are strictly pass/fail – either the user is positively identified or not. This is not risk mitigation, but risk avoidance, which is not necessarily a bad concept. The problem with the concept of risk avoidance is that there is a fine line where a marginal False Rejection Rate[3] results in customer dissatisfaction, and acceptable FRRs will be different for every user.

A Fluid Solution

The design of keystroke biometrics balances the FFIEC guidance principles of risk mitigation with customer satisfaction.

One area which the report covered briefly is the use of secondary authentication as part of a more refined risk mitigation policy; that is, using secondary measures to provide users tiered access to their accounts. Tiered access (based on secondary authentication results) provides a better balance between customer satisfaction and risk mitigation. One technique for implementing this tiered design is through behavioral biometrics.

Behavioral biometrics is an area of biometrics well out of the media spotlight. It is a different breed of security. Whereas physical biometrics, such as fingerprint and iris recognition, measures a biological aspect of a user; behavioral biometrics measures the behavioral patterns of a user. Speech verification, handwriting recognition and keystroke biometrics are well known variations[4]. Rather than giving an absolute pass/fail measurement, these behavioral biometrics result in dynamic confidence measurements. Behavioral biometrics solutions provide:

- Intangible Tokens: Like all biometric solutions, behavioral biometrics does not require a user to carry yet another USB dongle, FOB or other extraneous authentication token. The user is the token.

- Limited User Liability: In the world of biometrics, the theft of your fingerprint can be not only devastating, but irreversible. Behavioral biometrics, like all secondary authentication methods, is token-driven. The token, for example in keystroke biometrics, is the pattern of typing surrounding your userid/password combination. If the token is ever compromised, simply register a new token – i.e. the typing pattern around a different password.

- True Risk Mitigation: The use of confidence measurements allows levels of access to be obtained. For example, a high confidence match has no restrictions, whereas a mid-level match may restrict large transactions and password changes, and a very low-rated match may present the user with additional customer verification techniques.

One such behavioral biometric technology, keystroke biometrics, provides a fluid solution to secondary authentication; it allows the user to use normal behavior to access their account and

[3] False Rejection Rate, or FRR, is the refusal of a valid user because of various reasons: user error, input device malfunction or other external circumstances.
[4] More interesting variations include gait analysis and speech removal analysis.

provides a seamless secondary authentication interface. Keystroke biometrics technology provides:

- Seamless Operation: The keystroke biometric data is captured as the user types their login information; there are no secondary steps to perform.

- Ubiquitous Access: Unlike other biometrics, it uses only a standard keyboard and client software is downloaded on demand – so it can be accessed virtually anywhere.

- Cost Effective Deployment: Among the list of obstacles to implementing a robust online user verification system, any system that requires special hardware will not be a cost effective solution. In the realm of behavioral biometrics, only keystroke biometrics offers a software-only solution. Because there is no hardware to maintain and the cost per user is substantially lower compared to other multi-factor solutions; keystroke biometrics provides a compelling economic business case.

The use of keystroke biometrics along with proper access control policies, logging and auditing can create a cost-efficient and truly reasonable solution to the FFIEC guidance principles on internet banking authentication. Not only can it provide for the existing top 100 enterprise customers, but also allows expansion to all customers – especially those multitudes of less profitable customers the identity thieves frequently target.

Summary

The FFIEC has created an initiative where enterprise e-business is measured not simply by corporate liability but by the protection of the enterprise customer. Although the guidance may be missing a legislative bite, it is prudent for the financial institutions to plan an implementation path for multi-factor online authentication within this fiscal year.

John C. Checco [CISSP] is a member of ASIS NY, Infragard NY, (ISC)2, the *WSTA Advisory/Content Committee* and president of bioChec™. Feel free to end comments to checco@checco.com.